IN THE UNITED STATES DISTRICT COURT FOR THE
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

GILBERT HALE, LYNDA HALE, and ALAN WOOTEN, individually and on behalf of all others similarly situated, Plaintiffs, v. GENWORTH FINANCIAL, INC., Defendant.	Case No.: 3:23-cv-517 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Gilbert Hale, Lynda Hale, and Alan Wooten (collectively, "Plaintiffs"), by and through their undersigned counsel, bring this Class Action Complaint against Defendant Genworth Financial, Inc. ("Genworth" or "Defendant") individually and on behalf of all others similarly situated, and alleges as follows, based upon personal knowledge as to themselves, and upon information and belief as to all other matters.

INTRODUCTION

1. Plaintiffs bring this action on behalf of themselves and all other individuals similarly situated ("Class Members") against Genworth for its failure to secure and safeguard the personally identifiable information ("PII") of at least 2.5 million individuals who are either customers or insurance agents of the company.

2. Genworth, headquartered in Richmond, Virginia, provides life insurance, long-term care insurance, mortgage insurance, and annuities. In the regular course of its business, Genworth contracts with vendors to handle highly-sensitive policyholder and insurance agent information.

3. One such vendor is Pension Benefit Information, LLC, dba PBI Research Services

("PBI"), which Genworth uses to identify deaths of policyholders and insurance agents to whom it pays commissions. In the course of its business, Genworth transferred the highly-sensitive personal information of millions of individuals to PBI, which utilized a file transfer service called MOVEit, marketed and offered by Progress Software Corporation ("PSC").

4. On June 16, 2023, PBI "advised Genworth that specific Genworth files containing policyholder and agent information were compromised due to a security event that took advantage of a vulnerability identified in the widely-used MOVEit file transfer software that PBI uses." [1] PBI admitted that the "security event" was a targeted attack by the CL0P ransomware gang (the "Data Breach").[2]

5. The Data Breach "started on May 27th, 2023, when the Cl0p ransomware gang began exploiting a MOVEit Transfer zero-day vulnerability to allegedly steal data from hundreds of companies. [Thereafter], the Cl0p gang began extorting companies by slowly listing impacted organizations on its data leak site as they attempt to pressure victims to pay a ransom demand."[3]

6. Genworth estimates that the Data Breach occurred between May 29 and May 30, 2023, and exposed individuals' Social Security numbers, first and last names, dates of birth, zip codes, states of residence, policy numbers, the role of the individual (ex. Annuitant, Joint Insured, Owner, etc.), and the general product type. If deceased, the exposed information included the city and date of death, along with the source of that information. For agents, the exposed information includes Social Security numbers, first and last names, dates of birth, and full addresses. If

[1] *Id.*

[2] https://www.pbinfo.com/faq-communication/ "According to public reporting and security researchers, the "CL0P" threat actor group is claiming responsibility for this event." (last visited August 15, 2023).

[3] https://www.bleepingcomputer.com/news/security/moveit-breach-impacts-genworth-calpers-as-data-for-32-million-exposed/ (last visited August 15, 2023).

deceased, the exposed information also included dates of death and the source of that information.[4]

7. Genworth owed a non-delegable duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure.

8. Genworth could have prevented the Data Breach by properly vetting and monitoring the systems of its third-party vendors, including PBI and its use of a highly vulnerable file transfer software MOVEit.

9. Plaintiffs and Class members entrusted Genworth with, and allowed Genworth to gather, highly sensitive information as part of obtaining financial and insurance services. They did so in confidence, and they had the legitimate expectation that Genworth would respect their privacy and act appropriately, including only sharing their information with vendors and business associates who legitimately needed the information and were equipped to protect it through having adequate processes in place to safeguard it.

10. Trust and confidence are key components of Plaintiffs' and Class Members' relationship with Genworth. Without it, Plaintiffs and Class Members would not have provided Genworth with, or allowed Genworth to collect, their most sensitive information in the first place. To be sure, Plaintiffs and Class Members relied upon Genworth to keep their information secure, as it is required by law to do.

11. Genworth breached its non-delegable duty to Plaintiffs and Class Members by, among other things, failing to implement and maintain reasonable security procedures and practices to protect the PII entrusted to it from unauthorized access and disclosure, including by

[4] https://www.genworth.com/moveit.html (last visited August 15, 2023).

ensuring its vendors and business associates had secure services, processes and procedures in place to safeguard PII that Genworth shared with those third parties.

12. As a result of Genworth's breach of its non-delegable duty, victims of the Data Breach are at serious risk. Their most sensitive personal PII is in the possession of a well-known cybercriminal group seeking to profit from it in any number of ways that will expose them to identify theft, fraud, and financial harms for years to come.

13. Plaintiffs bring this action on behalf of themselves and those similarly situated to seek redress for the lifetime of harm they will now face, including but not limited to reimbursement of losses associated with identity theft and fraud, out-of-pocket costs incurred to mitigate the risk of future harm, compensation for time and effort spent responding to the Data Breach, the costs of extended credit monitoring services and identity theft insurance, and injunctive relief requiring Genworth to ensure that its third-party vendors implement and maintain reasonable data security practices going forward.

PARTIES

14. Plaintiffs Gilbert and Lynda Hale are residents and citizens of New York, whose Personal Information was compromised in the Data Breach.

15. Plaintiff Alan Wooten is a resident and citizen of Arkansas, whose Personal Information was compromised in the Data Breach.

16. Defendant Genworth Financial, Inc. is a Virginia corporation, with its principal place of business at 6620 W Broad St, Richmond, Virginia, 23230.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d), because this is a class action in which at least one member of the class is a citizen of a state different from Defendant, the amount in controversy exceeds $5

million exclusive of interest and costs, and the proposed class contains more than 100 members.

18. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(b)(2) and (c)(2) because a substantial part of the events or omissions giving rise to the claim occurred here and Genworth is subject to this Court's personal jurisdiction. Among other things, Genworth is headquartered in this District, Genworth conducts substantial business operations in this District, and Genworth purposely availed itself to the benefits of this jurisdiction.

FACTUAL ALLEGATIONS

Genworth's Privacy Practices

19. Genworth advertises that it provides financial and insurance services to help its customers "navigate caregiving options, protect and grow their retirement income, and prepare for financial challenges that come as we age."[5]

20. In the course of these services, Genworth collects and maintains patients' highly sensitive PII, including, but not limited to their Social Security numbers, first and last names, dates of birth, zip codes, states of residence, policy numbers, cities, and dates of death, where applicable.

21. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Genworth assumed legal and equitable duties and knew or should have known it was responsible for protecting the PII from unauthorized disclosure.

22. Genworth understands the importance of protecting its customers' and insurance agents' PII and maintains a Privacy Policy confirming such. According to Genworth's Privacy Policy, it complies with "[f]ederal and State requirements related to the protection and use of your data. This means that we only share data where we are permitted or required to do so. We also may

[5] https://www.genworth.com/about-us.html (last visited August 15, 2023).

be required to obtain your authorization before disclosing certain types of personal data."[6]

23. Genworth further states that it does "not sell personal data about current or former customers or their accounts. We do not share your personal data for marketing purposes with anyone outside our family companies. When affiliates or outside companies perform a service on our behalf, we may share your personal data with them. We require them to protect your personal data, and we only permit them to use your personal data to perform these services."[7]

24. Genworth also maintains a "Code of Ethics," which "contains the core policies that govern [employees] work, as well as an outline of [their] responsibilities in upholding the Code and protecting it."[8] With regard to customer information, Genworth's Code of Ethics states that "[o]ur customers, distributors, employees, and other individuals have entrusted sensitive personal data to us with the full expectation that we will exercise the appropriate degree of care in handling and storing it. . . . Many of us have access to information that is sensitive in nature and confidential. Confidential information includes non-public information that might be useful to our competitors, or harmful to the Company or its customers, if disclosed. . . . Genworth is committed to (1) handling and storing all sensitive personal data responsibly and in full compliance with applicable privacy laws, and (2) maintaining the confidentiality of property or other sensitive information, as appropriate."[9]

25. Genworth further states that "[i]f Genworth will need to disclose sensitive personal data to a supplier or other third party, partner with an internal legal counsel, a compliance officer,

---

[6] https://pro.genworth.com/riiproweb/productinfo/pdf/45242.pdf (last visited August 15, 2023).

[7] *Id*.

[8] https://pro.genworth.com/riiproweb/productinfo/pdf/GF90384.pdf (last visited August 15, 2023).

[9] *Id.*

data security team member, or a sourcing representative to (1) assess the supplier's security safeguards, and (2) include adequate legal protections. . . . Disclosures to a third party should be limited to the minimum necessary to accomplish the intended purpose."[10]

26. Despite recognizing its duty to do so, Genworth failed to assess and monitor its third-party vendor's security safeguards to protect Plaintiffs' and Class Members' PII.

27. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Genworth to keep their PII confidential and maintained securely, to use this information for business purposes only, to make only authorized disclosures of this information, and to ensure that its third-party vendors take similar steps.

The Data Breach

28. According to a data breach notice sent by PBI on behalf of Genworth ("Breach Notice"), an unauthorized party accessed one of PBI's MOVEit Transfer servers on May 29, 2023 and May 30, 2023, exploiting a glaring vulnerability in the software, and downloading highly sensitive PII of at least 2.5 million Genworth customers and insurance agents stored on its servers, including Social Security numbers, first and last names, dates of birth, zip codes, states of residence, policy numbers, cities, and dates of death, where applicable.

29. The Breach Notice further provided that "[w]e take this event and the security of information in our care seriously. Upon learning about this vulnerability, we promptly took steps to patch servers, investigate, assess the security of our systems, and notify potentially affected customers and individuals associated with those customers. In response to this event, we are also reviewing and enhancing our information security policies and procedures."

30. In a report filed with the Securities and Exchange Commission, Genworth

[10] *Id*.

described its discovery of the Data Breach as follows:

> Genworth Financial, Inc. (the "Company") has been notified by PBI Research Services ("PBI"), a third-party vendor to the Company, that PBI, in common with numerous other organizations and governmental agencies, was subject to the widely reported security events involving the MOVEit file transfer system, which PBI uses in the performance of its services. The MOVEit file transfer system security event resulted in the unauthorized acquisition by a third-party of data from several organizations and governmental agencies, including Company data. As further described below, the Company believes that the personal information of a significant number of insurance policyholders or other customers of its life insurance businesses was unlawfully accessed, and is working to ensure that protection services are provided to those impacted individuals.[11]

26. Genworth also posted a Security Event Notice ("Security Notice") on its website that vaguely discusses the Data Breach and imprecisely addresses the steps taken to ensure a Data Breach of this kind does not happen again: "At Genworth, we have implemented technical, physical, and process safeguards to maintain the confidentiality of customer information. Further, we require third parties that receive and store the personal information of our customers to take similar steps, and we work to understand the measures they have taken. While the MOVEit event has impacted various organizations globally, Genworth will continue to focus on and seek opportunities to improve how third parties protect the data of our customers."[12]

27. Absent from the Breach Notice and Security Notice are any details regarding how the Data Breach happened, what Genworth did in response to the ransom demand, or how Genworth's actions have remediated the root cause of the Data Breach.

The Data Breach was Preventable

28. As noted above, following the Data Breach, Genworth stated that has "implemented technical, physical, and process safeguards to maintain the confidentiality of customer information

[11] https://investor.genworth.com/sec-filings/all-sec-filings/content/0001193125-23-172549/d463993d8k.htm (last visited 8/15/2023).

[12] https://www.genworth.com/moveit.html (last visited 8/15/2023).

[and requires] third parties that receive and store the personal information of our customers to take similar steps."[13]

29. Had Genworth ensured that PBI maintained industry-standard safeguards to monitor, assess, and update security controls and related system risks, Genworth could have ensured that sensitive customer and agent data was not transferred to a vendor that was unequipped to protect it. Genworth's lack of oversight of PBI's security controls, and PBI's implementation of enhanced security measures only after the Data Breach are inexcusable.

28. Genworth was at all times fully aware of its obligation to protect its customers' and insurance agents' PII and the risks associated with failing to do so. Genworth observed frequent public announcements of data breaches affecting finance and insurance industries and knew that information of the type collected, maintained, and stored by Genworth is highly coveted and a frequent target of hackers.

29. Indeed, insurance institutions are prime targets for cyberattacks because of their size and scope, along with the substantial amount of sensitive data they manage and store. There have been at least three major insurance related data breaches in the United States since the beginning of this year, some also perpetrated by the CL0P ransomware gang.[14]

30. For example, in April 2023, NationsBenefits "disclosed that thousands of its members had their personal information compromised in a late-January ransomware attack targeting Fortra's GoAnywhere platform, a file-transfer software that the firm was using. According to news reports, ransomware gang Cl0p claimed responsibility for the attack, saying it

[13] *Id*.

[14] https://www.insurancebusinessmag.com/us/guides/the-insurance-industry-cyber-crime-report-recent-attacks-on-insurance-businesses-448429.aspx (last visited August 15, 2023).

took advantage of a previously unknown vulnerability "[15]

31. In mid-April 2023, "the second-largest health insurer [Point32Health] in Massachusetts suffered major technical outages resulting from a ransomware attack. The incident brought down the company's systems that it uses to service members and providers, resulting in some members having difficulty contacting their insurers."[16]

32. In May 2023, MCNA Insurance Company disclosed that "personal health information of nearly nine million patients was compromised in a cyber incident discovered in March. In a data breach notification letter filed with the Maine state attorney general's office dated May 26, the firm said that it detected unauthorized access to its systems on March 6, with some found to be infected with malicious code. . . . According to MCNA, the hackers were successful in accessing patient personal information."[17]

33. Moreover, ransomware attacks are especially prevalent in the insurance industry.[18] For years federal agencies have warned about the increasing risk of ransomware attacks on companies holding PII. For example, in October 2019 the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[19]

34. In April 2020, ZDNet reported in an article titled "Ransomware mentioned in

---

[15] *Id*.

[16] *Id.*

[17] *Id*.

[18] *Id*.

[19] https://www.ic3.gov/Media/Y2019/PSA191002 (last visited August 15, 2023).

1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for complaints as revenge against those who refuse to pay."[20]

35. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[21]

36. At all relevant times, Genworth knew, or reasonably should have known, of the importance of safeguarding PII and the foreseeable consequences that would occur if its vendor's data security systems were breached, including, specifically, the significant costs that would be imposed on affected individuals as a result of the breach.

37. Despite all the publicly available knowledge of the serious threat of compromises of PII and despite holding and transferring the PII of millions of individuals, Genworth failed to use reasonable care in maintaining and overseeing the privacy and security of Plaintiffs' and Class Members' PII. Had Genworth used reasonable and adequate due diligence in assessing and monitoring the security protocols of its vendors, cybercriminals never would have accessed the PII of millions of Genworth policyholders and agents.

Allegations Relating to Plaintiffs

38. Plaintiffs Gilbert and Lynda Hale live and reside in Pittsford, New York and are

[20] https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited August 15, 2023).
[21] https://www.cisa.gov/sites/default/files/2023-01/CISA_MS
- ISAC_Ransomware%20Guide_S508C.pdf (last visited August 15, 2023).

long-term care policyholders with Genworth.

39. Plaintiff Alan Wooten lives in Fayetteville, Arkansas and is also a long-term care policyholder with Genworth.

40. To obtain insurance benefits from Genworth, Plaintiffs provided Genworth with highly-sensitive PII, including but not limited to demographic and financial information.

41. Following the Data Breach, Plaintiffs received a Breach Notice from PBI, on behalf of Genworth, dated July 14, 2023, notifying them of a "third-party software event that affected the security of some of [their] information."

42. Specifically, the Breach Notice stated that "[o]ur investigation determined that the following types of information related to you were present in the server at the time of the event: name, Social Security number, date of birth, zip code, state of residence, role in policy/account (eg., Annuitant, Joint Insured, Owner, etc.), general product type, and the policy/account number."

43. The letter advised Plaintiffs to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and detect errors for the next twelve to twenty-four months and report suspected identity theft incidents to the insurance company."

44. As a result of the Data Breach, Plaintiffs have spent time and effort researching the breach and reviewing their financial accounts and bank statements for evidence of unauthorized activity, which they will continue to do indefinitely. Plaintiffs have also suffered emotional distress knowing that their highly sensitive information is no longer confidential and can be used for blackmail, extortion, identity theft or fraud, and any number of additional harms against them for the rest of their lives.

45. Genworth continues to store Plaintiffs' PII on its internal systems, and share

Plaintiffs' PII with its third-party vendors. Thus, Plaintiffs have a continuing interest in ensuring that their PII is protected and safeguarded from future breaches.

Genworth Failed to Comply with Federal Law and Regulatory Guidance

46. Federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For example, the Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.[22]

47. The FTC's publication *Protecting Personal Information: A Guide for Business* sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data.[23] Among other things, the guidelines note that businesses should (a) protect the personal customer information that they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their networks' vulnerabilities; and (e) implement policies to correct security problems. The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[24]

48. Additionally, the FTC recommends that organizations limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security,

[22] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited August 15, 2023).

[23] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited August 15, 2023).

[24] *Id*.

monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[25]

49. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[26]

50. Genworth was fully aware of its obligation to implement and use reasonable measures to protect the PII of its customers and insurance agents but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring. Genworth's failure to employ reasonable measures to protect against unauthorized access to patient information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Genworth is Subject to the Gramm-Leach-Bliley Act

51. Genworth is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

52. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

[25] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited August 15, 2023).

[26] https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited August 15, 2023).

53. Genworth collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Genworth was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1 *et seq*., and is subject to numerous rules and regulations promulgated under the GLBA statutes.

54. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of consumer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of consumer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of consumer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Genworth violated the Safeguard Rule.

55. Genworth's conduct resulted in a failure to follow GLBA mandated rules and regulations, many of which are also industry standard. In particular, the Data Breach demonstrates that PBI failed to implement (or inadequately implemented) information security policies or procedures to protect the confidentiality of the Personal Information it maintained in its data systems. The Data Breach further demonstrates that Genworth failed to oversee PBI and to require

PBI to protect the security and confidentiality of its customers' and insurance agents' Personal Information.

The Impact of Data Breach on Victims

56. Genworth's failure to keep Plaintiffs' and Class Members' PII secure has severe ramifications. Given the highly sensitive nature of the PII stolen in the Data Breach— Social Security numbers, first and last names, dates of birth, zip codes, states of residence, and policy numbers, etc.—hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future. As a result, Plaintiffs have suffered injury and face an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

57. The PII exposed in the Data Breach is highly-coveted and valuable on underground markets. Identity thieves can use the PII to: (a) commit insurance fraud; (b) obtain a fraudulent driver's license or ID card in the victim's name; (c) obtain fraudulent government benefits; (d) file a fraudulent tax return using the victim's information; (e) commit medical and healthcare-related fraud; (f) access financial and investment accounts and records; (g) engage in mortgage fraud; or (h) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

58. Further, malicious actors often wait months or years to use the PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PII, meaning individuals can be the victims of several cybercrimes stemming from a single data breach.

59. Given the confirmed exfiltration of Genworth's customers' and insurance agents' PII from PBI' systems, many victims of the Data Breach have likely already experienced significant harms as the result of the Data Breach, including, but not limited to, identity theft and

fraud. Plaintiffs and Class Members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit monitoring services, reviewing financial and insurance statements, checking credit reports, and spending time and effort searching for unauthorized activity.

60. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2021 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 84% reported anxiety;
- 76% felt violated;
- 32% experienced financial related identity problems;
- 83% reported being turned down for credit or loans;
- 32% reported problems with family members as a result of the breach;
- 10% reported feeling suicidal.[27]

61. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate/lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and

[27] https://www.idtheftcenter.org/wp-content/uploads/2021/09/ITRC_2021_ Consumer_Aftermath _Report.pdf (last visited August 15, 2023).

- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[28]

49. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

50. The unauthorized disclosure of Social Security Numbers can be particularly damaging because Social Security numbers cannot be easily replaced. In order to obtain a new number, a person must prove, among other things, he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until the damage has been done. Furthermore, as the Social Security Administration warns:

> A new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit reporting companies use the number, along with other Personal Information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other Personal Information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you will not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit

[28] https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last visited August 15, 2023).

history under the new number may make it more difficult for you to get credit.[29]

62. The unauthorized disclosure of the sensitive PII to data thieves also reduces its inherent value to its owner, which has been recognized by courts as an independent form of harm.[30]

63. Consumers are injured every time their data is stolen and traded on underground markets, even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that can be aggregated together or accessed by different criminal actors who intend to use it for different fraudulent purposes. Each data breach increases the likelihood that a victim's personal information will be exposed to more individuals who are seeking to misuse it at the victim's expense.

64. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and Class Members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. the unconsented disclosure of confidential information to a third party;

b. unauthorized use of their PII without compensation;

c. losing the value of the explicit and implicit promises of data security;

d. losing the value of access to their PII permitted by Genworth without permission;

e. identity theft and fraud resulting from the theft of their PII;

f. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

---

[29] Social Security Administration, *Identity Theft and Your Social Security Number* (June 2017), http://www.ssa.gov/pubs/10064.html (last visited August 15, 2023).

[30] *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

g. anxiety, emotional distress, and loss of privacy;

h. the present value of ongoing credit monitoring and identity theft protection services necessitated by the Data Breach;

i. unauthorized charges and loss of use of and access to their accounts;

j. lowered credit scores resulting from credit inquiries following fraudulent activities;

k. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

l. the continued, imminent, and certainly impending injury flowing from potential fraud and identify theft posed by their PII being in the possession of one or many unauthorized third parties.

65. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[31]

66. There may also be a significant time lag between when personal information is stolen and when it is misused for fraudulent purposes. According to the Government Accountability Office, which conducted a study regarding data breaches: "law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to

[31] E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov. 14, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited August 15, 2023).

measure the harm resulting from data breaches cannot necessarily rule out all future harm."[32]

67. Plaintiffs and Class Members place significant value in data security. According to a survey conducted by cyber-security company FireEye Mandiant, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more to work with a provider that has better data security. Seventy percent of consumers would provide less personal information to organizations that suffered a data breach.[33]

68. Plaintiffs and Class Members have a direct interest in Genworth's promises and duties to protect their PII, i.e., that Genworth *not increase* their risk of identity theft and fraud. Because Genworth failed to live up to its promises and duties in this respect, Plaintiffs and Class Members seek the present value of ongoing identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by Genworth's wrongful conduct. Through this remedy, Plaintiffs seeks to restore themselves and Class Members as close to the same position as they would have occupied but for Genworth's wrongful conduct, namely its failure to adequately protect Plaintiffs' and Class Members' PII.

69. Plaintiffs and Class Members further seek to recover the value of the unauthorized access to their PII permitted through Genworth's wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's PII is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a Plaintiffs may generally recover the

[32] https://www.gao.gov/assets/gao-07-737.pdf (last visited August 15, 2023).

[33]https://web.archive.org/web/20220205174527/https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited August 15, 2023).

reasonable use value of the IP—i.e., a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a nonpracticing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiffs and Class Members have a protectible property interest in their PII; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, *i.e.,* evidence regarding the value of similar transactions.

70. Plaintiffs and Class Members have an interest in ensuring that their PII is secured and not subject to further theft because Genworth continues to hold their PII.

CLASS ACTION ALLEGATIONS

71. Plaintiffs seek relief individually and as a representative of all others who are similarly situated. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3) and/or (c)(4), Plaintiffs seeks certification of a nationwide class defined as: All U.S. persons whose PII was compromised as a result of the Data Breach announced by Genworth between May 29, 2023 and May 30, 2023 (the "Class").

72. Excluded from the Class are Defendant, any entity in which Genworth has a controlling interest, and Genworth's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded are all persons who make a timely election to be excluded from the Class and any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

73. **Ascertainability.** The members of the Class are readily identifiable and ascertainable. Genworth and/or its affiliates, among others, possess the information to identify and

contact Class Members.

74. **Numerosity. Fed. R. Civ. P. 23(a)(1).** The members of the Class are so numerous that joinder of all of them is impracticable. Genworth's statements reveal that the Class contains at least 2.5 million individuals whose PII was compromised in the Data Breach.

75. **Commonality. Fed. R. Civ. P. 23(a)(2) and 23(b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include, but are not limited to:

a. Whether Genworth owed Plaintiffs and Class Members a duty to implement and maintain reasonable security procedures and practices to protect their PII;

b. Whether Genworth acted negligently in connection with the monitoring and/or protection of Plaintiffs' and Class Members' PII;

c. Whether Genworth violated its non-delegable duty to implement reasonable security systems to protect Plaintiffs' and Class Members' PII;

d. Whether Genworth's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiffs and Class Members; and

e. Whether Plaintiffs and Class Members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

76. Genworth has engaged in a common course of conduct and Plaintiffs and Class Members have been similarly impacted by Genworth's failure to maintain reasonable security procedures and practices to protect customers' and insurance agents' PII, and to adequately monitor and audit the data security of its third-party vendors and business associations.

77. **Typicality. Fed. R. Civ. P. 23(a)(3).** As to the Class, Plaintiffs' claims are typical of the claims of the members because all Class Members had their PII compromised in the Data Breach and were harmed as a result.

78. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs have no known interest antagonistic to those of the Class and their interests are aligned with Class Members' interests. Plaintiffs were subject to the same Data Breach as Class Members, suffered similar harms, and faces similar threats due to the Data Breach. Plaintiffs have also retained competent counsel with significant experience litigating complex class actions, including data breach cases.

79. **Superiority. Fed. R. Civ. P. 23(b)(3).** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most if not all Class Members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members and risk inconsistent treatment of claims arising from the same set of facts and occurrences. Plaintiffs know of no difficulty likely to be encountered in the maintenance of this action as a class action under the applicable rules.

80. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

81. Likewise, particular issues are appropriate for certification under Rule 23(c)(4) because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether Genworth owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, and safeguarding their PII;

b. Whether Genworth failed to take reasonable steps to safeguard the PII of Plaintiffs and Class Members;

c. Whether Genworth failed to implement and maintain reasonable security procedures and practices to protect the PII entrusted to it from unauthorized access and disclosure, including by ensuring their vendors and business associates had secure services, processes and procedures in place to safeguard PII that Genworth shared with its third-parties.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(*On Behalf of Plaintiffs and the Class*)

82. Plaintiffs repeat and reallege every allegation set forth in the paragraphs 1 through 70.

83. Genworth owed a duty to Plaintiffs and Class Members to exercise reasonable care in safeguarding and protecting their PII in Genworth's possession, custody, or control, including non-delegable duties to safeguard that PII. This duty could not be delegated to Genworth's vendors and business associates; rather, Genworth had an independent obligation to control all environments into which it placed customers' and insurance agents' PII, and to ensure that those environments were used, configured, and monitored in such a way as to ensure the safety of its customers' and insurance agents' data.

84. Genworth owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, security, safeguarding, storing, and protecting Plaintiffs' and Class Members' PII within their control from being compromised, lost, stolen, accessed and misused by unauthorized persons.

85. Genworth owed a duty of care to Plaintiffs and Class Members to provide reasonable security, consistent with industry standards, to ensure that its systems and networks

adequately protect the PII of customers and insurance agents.

86. Genworth had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust Genworth with their PII as a condition of obtaining financial and insurance services was predicated on the understanding that Genworth would take adequate security precautions to protect their PII.

87. Genworth's duties to use reasonable care in protecting PII also arise from common law and statutes and regulations such as the FTC Act and GLBA, as well as their own promises regarding privacy and data security.

88. Genworth breached its common law duty to act with reasonable care in collecting and storing customers' and insurance agents' PII, which exists independently from any contractual obligations between the parties. Specifically, Genworth breached its common law, statutory, and other duties to Plaintiffs and Class Members in numerous ways, including by:

a. failing to exercise reasonable oversight of the vendors it entrusted with highly-sensitive PII;

b. failing to comply with industry standard data security standards during the period of the Data Breach;

c. failing to comply with regulations protecting the PII at issue during the period of the Data Breach;

d. failing to adequately monitor and audit the data security of its vendors and business associates such as PBI;

e. failing to adequately monitor, evaluate, and ensure the security of PBI's network and systems;

f. failing to recognize in a timely manner that Plaintiffs' and Class Members' PII had been compromised; and

g. failing to timely and adequately disclose critical information regarding the nature of the Data Breach.

89. Genworth owed a non-delegable duty of care to Plaintiffs and members of the Class

because they were foreseeable and probable victims of inadequate security practices. Genworth knew or should the risks of collecting and storing Plaintiffs' and all other Class Members' PII and the importance of maintaining secure systems and ensuring their vendors and business associates with whom Genworth shared individuals' PII—such as PBI—had secure services, processes and procedures in place to safeguard that PII. Genworth knew it was a target of cyberattacks and the critical importance of adequately securing customers' and insurance agents' PII.

90. Plaintiffs Class Members entrusted Genworth with their PII with the understanding that Genworth would safeguard their information.

91. But for Genworth's negligent conduct and breach of its duties owed to Plaintiffs and Class members, their PII would not have been compromised.

92. As a direct and proximate result of Genworth's conduct, Plaintiffs and the Class have and will suffer damages including, but not limited to: (i) the uncompensated use of their PII by unauthorized parties; (ii) the publication and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in Genworth's possession and is subject to further unauthorized disclosures so long as Genworth fail to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the

rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by the Data Breach; (x) the value of the unauthorized access to their PII permitted by Genworth; and (xi) any nominal damages that may be awarded.

COUNT II
NEGLIGENCE *PER SE*
(*On Behalf of Plaintiffs and the Class*)

93. Plaintiffs repeat and reallege every allegation set forth in the paragraphs 1 through 70.

94. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. 15 U.S.C. § 45(a)(1).

95. Genworth violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs and Class Members' PII and by failing to comply with applicable industry standards. Genworth's conduct was particularly unreasonable given the sensitive nature of the PII they obtained and stored.

96. Genworth's duty to use reasonable security measures also arose under the GLBA, under which Genworth was required to ensure companies with whom it shared PII would use reasonable measures to secure it.

97. Genworth's violation of Section 5 of the FTC Act constitutes negligence *per se*.

98. Genworth's violation of the GLBA and its Safeguards Rule constitutes negligence *per se*.

99. Plaintiffs and Class Members are within the class of persons that the FTC Act and the GLBA were intended to protect.

100. The harm that occurred as a result of the Data Breach is the type of harm the FTC

Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class. The GLBA, with its Safeguard Rule, was similarly intended.

101. As a direct and proximate result of Genworth's negligence *per se*, Plaintiffs and Class Members have suffered, continue to suffer, and will suffer, injuries, damages, and harm as set forth herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT III
BREACH OF IMPLIED CONTRACT
(*On Behalf of Plaintiffs and the Class*)

102. Plaintiffs restate and re-allege every allegation set forth in paragraphs 1 through 70.

103. Plaintiffs and Class Members were required to provide their PII to Genworth in order to apply for and receive mortgage, life, and/or long-term care insurance.

104. Implicit in the agreement between Genworth and customers was the obligation that Genworth would implement and maintain reasonable safeguards to protect customers' information and comply with industry-standard data security practices.

105. Additionally, Genworth implicitly promised and agreed to retain this PII only under conditions that kept such information secure and confidential and only as long as reasonably necessary to perform essential business functions. As such, Genworth had a duty to reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or access.

106. Genworth breached its implied agreement with Plaintiffs and Class Members by sharing their information with third parties that failed to take appropriate measures to protect the confidentiality and security of their personal data, resulting in the Data Breach.

107. As a direct and proximate result of Genworth's conduct, Plaintiffs and members of the Class suffered injury and sustained actual losses and damages as described herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT IV
INVASION OF PRIVACY—INTRUSION UPON SELECTION
(*On Behalf of Plaintiffs and the Class*)

108. Plaintiffs restate and re-allege every allegation set forth in paragraphs 1 through 70.

109. Plaintiffs and Class Members shared PII with Genworth that Plaintiffs and Class Members wanted to remain private and non-public.

110. Plaintiffs and Class Members reasonably expected that the PII they shared with Genworth would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties or disclosed or obtained for any improper purpose.

111. Genworth's conduct as alleged above intruded upon Plaintiffs' and Class Members' seclusion under common law.

112. By intentionally disclosing Plaintiffs' and Class Members' PII to an unauthorized and unsecure third party, Genworth intentionally invaded Plaintiffs' and class members' privacy by:

a. intruding into Plaintiffs' and Class Members' private affairs in a manner that identifies Plaintiffs and Class Members and that would be highly offensive and objectionable to an ordinary person;

b. intentionally publicizing private facts about Plaintiffs and Class Members, which is highly offensive and objectionable to an ordinary person;

c. intentionally causing anguish or suffering to Plaintiffs and Class Members;
d. failing to adequately secure their PII from disclosure to unauthorized persons; and

e. enabling the disclosure of their PII without consent.

113. Genworth knew that an ordinary person in Plaintiffs' and Class Member's position would consider Genworth's intentional actions highly offensive and objectionable.

114. Genworth invaded Plaintiffs and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' seclusion by intentionally failing to safeguard, misusing, and/or disclosing their PII to PBI without their informed, voluntary, affirmative, and clear consent.

115. As a proximate result of such intentional misuse and disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted. Genworth's conduct, amounting to a substantial and serious invasion of Plaintiffs' and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Genworth's intentional actions or inaction highly offensive and objectionable.

116. In failing to protect Plaintiffs' and Class Members' PII, in intentionally misusing and/or disclosing their PII to PBI, an unauthorized party, Genworth acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private.

117. As a direct and proximate result of the foregoing conduct, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as described herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT V
BREACH OF CONFIDENCE
(*On Behalf of Plaintiffs and the Class*)

118. Plaintiffs restate and re-allege every allegation set forth in paragraphs 1 through 70.

119. In order to apply for and receive mortgage, life, and/or long-term care insurance, Plaintiffs and Class Members were required to provide their PII to Genworth. Such information

was highly personal, sensitive, and not generally known.

120. Genworth expressly and implicitly agreed to protect the confidentiality and security of the PII it collected, stored, and maintained.

121. Genworth's failure to adequately monitor and audit the data security of its vendors and business associates such as PBI resulted in disclosure of customers' and insurance agents' PII to unauthorized third parties.

122. As a direct and proximate result of Genworth's breach of confidence, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as described herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT VI
UNJUST ENRICHMENT
(*On Behalf of Plaintiffs and the Class*)

123. Plaintiffs restate and re-allege every allegation set forth in paragraphs 1 through 70.

124. Plaintiffs and Class Members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, used by, and maintained by Genworth and that was ultimately stolen in the Data Breach.

125. Genworth benefitted by the conferral upon it of the PII pertaining to Plaintiffs and the Class Members and by its ability to retain, use, and profit from that information. Genworth understood and valued this benefit. Genworth shared PII with PBI to monitor policyholders and agent deaths for purposes of maximizing its own profits.

126. Genworth also understood and appreciated that the PII pertaining to Plaintiffs and Class Members was private and confidential and its value depended upon Genworth maintaining the privacy and confidentiality of that PII.

127. Without Genworth's commitment to maintain the privacy and confidentiality of the

PII, that PII would not have been transferred to and entrusted to Genworth.

128. Because of Genworth's use of Plaintiffs' and Class Members' PII, Genworth sold more services and products than it otherwise would have. Genworth was unjustly enriched by profiting from the additional services and products they were able to market, sell, and create to the detriment of Plaintiffs and Class Members.

129. Genworth also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiffs' and Class Member's PII.

130. Genworth also benefited through their unjust conduct in the form of the profits they gained through the use of Plaintiffs' and Class Members' PII.

131. It is inequitable for Genworth to retain these benefits.

132. As a result of Genworth's wrongful conduct as alleged in this Complaint (including, among other things, its failure to oversee that its third-party vendors and business associations established and maintained adequate data security measures, its continued maintenance and use of the PII belonging to Plaintiffs and Class Members without adequately monitoring and auditing data security of its vendors and business associates, and its other conduct facilitating the theft of that PII), Genworth has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members.

133. Genworth's unjust enrichment is traceable to and resulted directly and proximately from the conduct alleged herein, including the compiling and use of Plaintiffs' and Class Members' sensitive PII, while at the same time failing to adequately monitor and audit the data security of its vendors and business associations in effort to maintain the information secure from intrusion and theft by hackers and identity thieves.

134. It is inequitable, unfair, and unjust for Genworth to retain these wrongfully obtained benefits. Genworth's retention of wrongfully obtained monies violates fundamental principles of justice, equity, and good conscience.

135. The benefit conferred upon, received, and enjoyed by Genworth was not conferred gratuitously, and it would be inequitable, unfair, and unjust for Genworth to retain the benefit.

136. Plaintiffs and Class Members have no adequate remedy at law.

137. Genworth are therefore liable to Plaintiffs and Class Members for restitution or disgorgement in the amount of the benefit conferred on Genworth as a result of its wrongful conduct, including specifically: the value to Genworth of the PII that was stolen in the Data Breach; the profits Genworth received and is receiving from the use of that information; the amounts that Genworth overcharged Plaintiffs and Class Members for use of Genworth's products and services; and the amounts that Genworth should have spent to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' PII.

COUNT VII
DECLARATORY JUDGMENT
(*On Behalf of Plaintiffs and the Class*)

138. Plaintiffs restate and re-allege every allegation set forth in paragraphs 1 through 70.

139. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

140. An actual controversy has arisen in the wake of the Data Breach regarding Genworth's present and prospective common law and other duties to reasonably safeguard PII and whether Genworth is currently maintaining data security measures adequate to protect Plaintiffs

and Class Members from further cyberattacks and data breaches that compromise their PII.

141. Genworth still possesses PII pertaining to Plaintiffs and Class Members, which means their PII remains at risk of further breaches because Genworth's data security measures—including monitoring and auditing data security of its vendors and business associates—remain inadequate. Plaintiffs and Class Members continue to suffer injuries as a result of the compromise of their PII and remain at an imminent risk that further compromises of their PII will occur in the future.

142. Pursuant to the Declaratory Judgment Act, Plaintiffs seeks a declaration that: (a) Genworth's existing data security measures do not comply with their obligations and duties of care; and (b) in order to comply with their obligations and duties of care, (1) Genworth must have policies and procedures in place to ensure the vendors and business associates with whom it shares sensitive PII maintain reasonable, industry-standard security measures, including, but not limited to, those listed at (ii), (a)-(i), *infra*, and must comply with those policies and procedures; (2) Genworth must: (i) purge, delete, or destroy in a reasonably secure manner Plaintiffs' and Class Members' PII if it is no longer necessary to perform essential business functions so that it is not subject to further theft; and (ii) implement and maintain reasonable, industry-standard security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Genworth's systems on a periodic basis, and ordering Genworth to promptly correct any problems or issues detected by such third-party security auditors, and ensure its third-party vendors and business associates engage in the same;

b. engaging third-party security auditors and internal personnel to run automated security monitoring, and ensure its third-party vendors and business associates engage in the same;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. encrypting PII and segmenting PII/HI by, among other things, creating firewalls and access controls so that if one area of Genworth's systems is compromised, hackers cannot gain access to other portions of Genworth's systems and ensure its third-party vendors and business associates perform the same;

e. purging, deleting, and destroying in a reasonable and secure manner PII not necessary to perform essential business functions and ensure its third-party vendors and business associates perform the same;

f. conducting regular database scanning and security checks, and ensure its third-party vendors and business associates conduct the same;

g. conducting regular employee education regarding best security practices and ensure its vendors and third-party business associations conduct the same;

h. implementing multi-factor authentication to combat system-wide cyberattacks and ensure its third-party vendors and business associates implement the same; and

i. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach, and ensure its third-party vendors and business associations conduct the same.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class Members, respectfully requests that the Court enter judgment in their favor and against Genworth as follows:

A. For an Order certifying the Class, as defined herein, and appointing Plaintiffs as the class representative and the undersigned counsel as class counsel;

B. For equitable relief enjoining Genworth from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Member's PII;

C. For equitable relief compelling Genworth to use industry-standard security methods and policies with respect to data collection, storage and protection, and sharing of information, and to dispose of Plaintiffs' and Class Members' PII in their possession that is not necessary to perform essential business functions;

D. For an award of damages, including nominal and statutory damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all claims so triable.

Date: August 15, 2023

Respectfully submitted,

/s/ Jonathan M. Petty
Jonathan M. Petty, VSB No. 43100
Michael G. Phelan, VSB No. 29725
Brielle M. Hunt, VSB No. 87652
PHELAN | PETTY PLC
3315 W. Broad St.
Richmond, VA 23230
Telephone: (804) 980-7100
jpetty@phelanpetty.com
mphelan@phelanpetty.com
bhunt@phelanpetty.com

Norman E. Siegel (*pro hac* vice forthcoming)
Brandi S. Spates (*pro hac vice* forthcoming)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
spates@stuevesiegel.com

Brian Douglas Penny (*pro hac* vice forthcoming)
GOLDMAN SCARLATO & PENNY, P.C.
Eight Tower Bridge, Suite 1025
161 Washington Street
Conshohocken, PA 19428
Tel. 484-342-0700
Fax 484-580-8747
penny@lawgsp.com

Stuart A. Davidson (*pro hac* vice forthcoming)
ROBBINS GELLER RUDMAN & DOWD LLP
255 NE Mizner Boulevard, Suite 720
Boca Raton, FL 33432
Telephone: (561) 750-3000
sdavidson@rgrdlaw.com

Attorneys for Plaintiffs and the Proposed Class